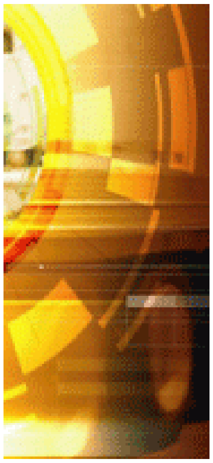
Michigan Department of State



Attachment D System Hardware & Software Overview & Recommendations For IRP System

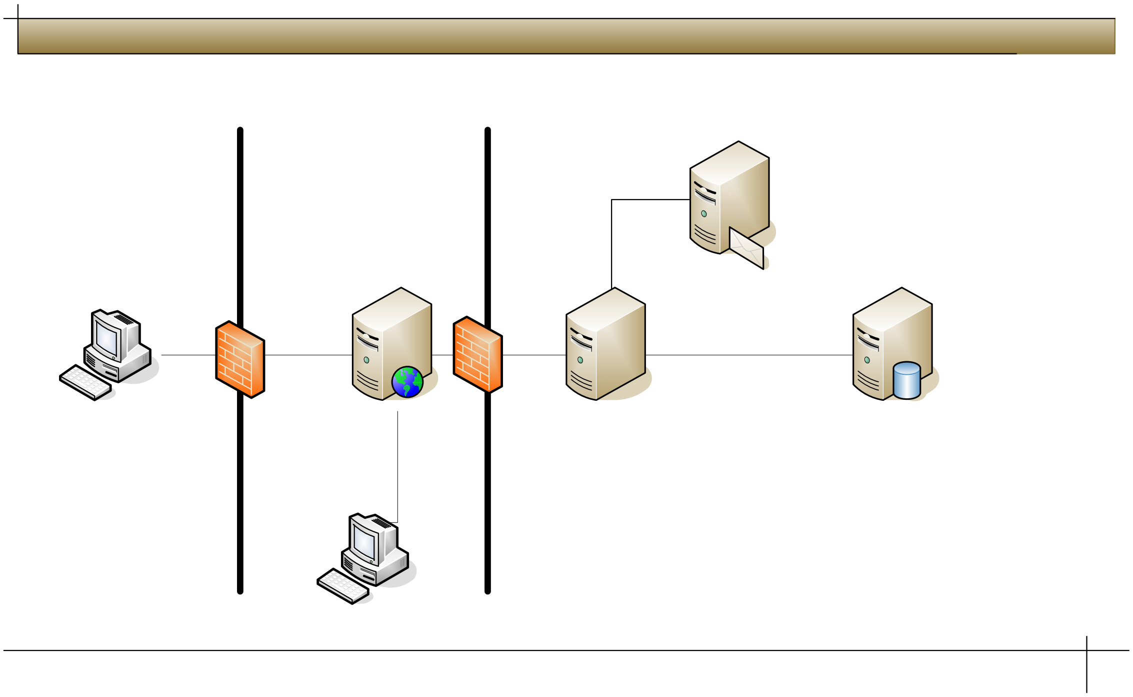
RFP #071I8200247

Submitted by Explore Information Services, LLC

Table of Contents

Explore IRP Configuration Recommendations

The simple network topology diagram shown below shows the minimum recommended Explore IRP configuration for Michigan.



The minimum recommended deployment model for the Michigan production environment consists of a single web server, single application server and a single database server.

From this model, adjustments can be made to support Michigan's business continuity requirements.   We start with the minimum deployment model so that it is clear what the foundation of the system requires in its fundamental state.

For the test environment in Michigan we recommend a similar set of servers. We highly recommend the use of VMware (or similar partitioning tools) for the web and app servers to save on the purchasing of hardware. For the database server we suggest creating a second database instance on the backup database server. With this in mind, the backup database server needs to have at least twice the disk space as the primary production server. The test database server can also be located on its own server if you would like to do so.

For the training environment we recommend another set of servers that are nearly a duplicate of the test environment.   To save expense, the State may want to consider using the test environment for the training environment and only have one set of servers. However, this can create conflicts between those testing and those in the training.

We recommend that Michigan purchase the hardware and software needed to support the three environments (testing, training, and production.) Explore will host development environments on our existing hardware. These environments are internal to Explore and are the base from which we promote our code to the test environment in Michigan.

Explore will assist Michigan with the process of ordering and installing the equipment. We offer to participate in the building of the purchase order, or at the very least, to review the purchase order it before it is submitted.

Once the hardware arrives we ask your engineers to rack the equipment, install the operating system, and other base software such as SQL Server on the database server. We provide recommended configuration settings to you for this step. Once this point is reached, we are able to install and configure the Explore system. We prefer to do this via a VPN connection. If needed, an onsite visit for initial installation is also an option.

Production Environment

Minimum Server Requirements	#	Description
Web Server	1	Duo Core 2.0 GHz Processors (or above) 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring such as NetIQ
Application Server	1	Duo Core 2.0 GHz Processors (or above) 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring such as NetIQ Anex 2D Barcode NetAddress 3.5 Active PDF Tool Kit
Primary Database Server	1	Duo Core 2.0 GHz Processors (or above) 8GB RAM 18 GB available for OS 300 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Standard Edition 2005 HW/SQ Monitoring
SMTP Server		We need access to an SMTP server to send automated email messages

Test (UAT) and Training Environments

Minimum Server Requirements	#	Description
VMWare Server (to save on physical hardware we recommend hosting the stage environment on a server that can host virtual machines)	1	Duo Core 2.0 GHz Processors (or above) 8GB RAM 300 GB available for virtual servers Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses VMWare ESX 2.x or greater
Virtual Web Server 1 server for testing 1 server for training	2	1GB RAM 18 GB available for OS 25-50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses Anex 2D Barcode NetAddress 3.5 Active PDF Tool Kit
Virtual Application Server 1 server for testing 1 server for training	2	1GB RAM 18 GB available for OS 25-50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses
Test Database Server	2	Duo Core 2.0 GHz Processors (or above) 8GB RAM 18 GB available for OS 300 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Standard Edition 2005 HW/SQ Monitoring *Note: This may coincide as a separate database instance on a backup database server for production.*
SMTP Server	1	We need access to an SMTP server to send automated email messages

Client-side Requirements

Client Requirements	#	Description
Desktop/Laptop System Minimum Requirements	N/A	Explore IRP recommends meeting the minimum's specified by the operating system and browser that you are using.
Recommended Web Browsers	N/A	Microsoft ® Internet Explorer 6.0+. Adobe ® Acrobat Reader Plug-in.
Operating System	N/A	Any operating system capable of using the browsers specified.

HTTPS/SSL	N/A	Required.
Office 2003 or later	N/A	This only applies to State users that need to work with generated correspondence and for audit worksheet upload/download. This is primarily the audit team.

Business Continuity Considerations

Business continuity needs to take into consideration a wide variety of items. For example, not only does redundancy need to be built into the computing platform, you need to take into account the relocation of workers, office equipment, etc. Because many of these considerations are out of our direct control, our business continuity considerations are focused on the computing equipment supporting the IRP system.

Web and Middle Tier Servers

Our typical recommendation for web and middle tier servers is to implement load balancers. One load balancer can manage one or more pairs of web and application servers. Another option is to have two load balancers with one managing traffic to the web servers and another managing traffic to the application servers. Having a load balanced environment provides several benefits. Most notably, one server can fail while the other server can continue to service the load without interruption. In addition, it provides an easy way to scale. Additional servers can be added with little effort. Last, it does provide some benefit when updating the system. For example, a web server can be taken out of production, have operating system patches applied, and then be slowly rationed into production to ensure that there are no problems.

Database Servers

We recommend the use of log shipping, clustering, or mirroring for having a business continuity option for the database server. Each option has its benefits. We will provide input to the Michigan team that is deciding the best architecture to build for Michigan purposes.

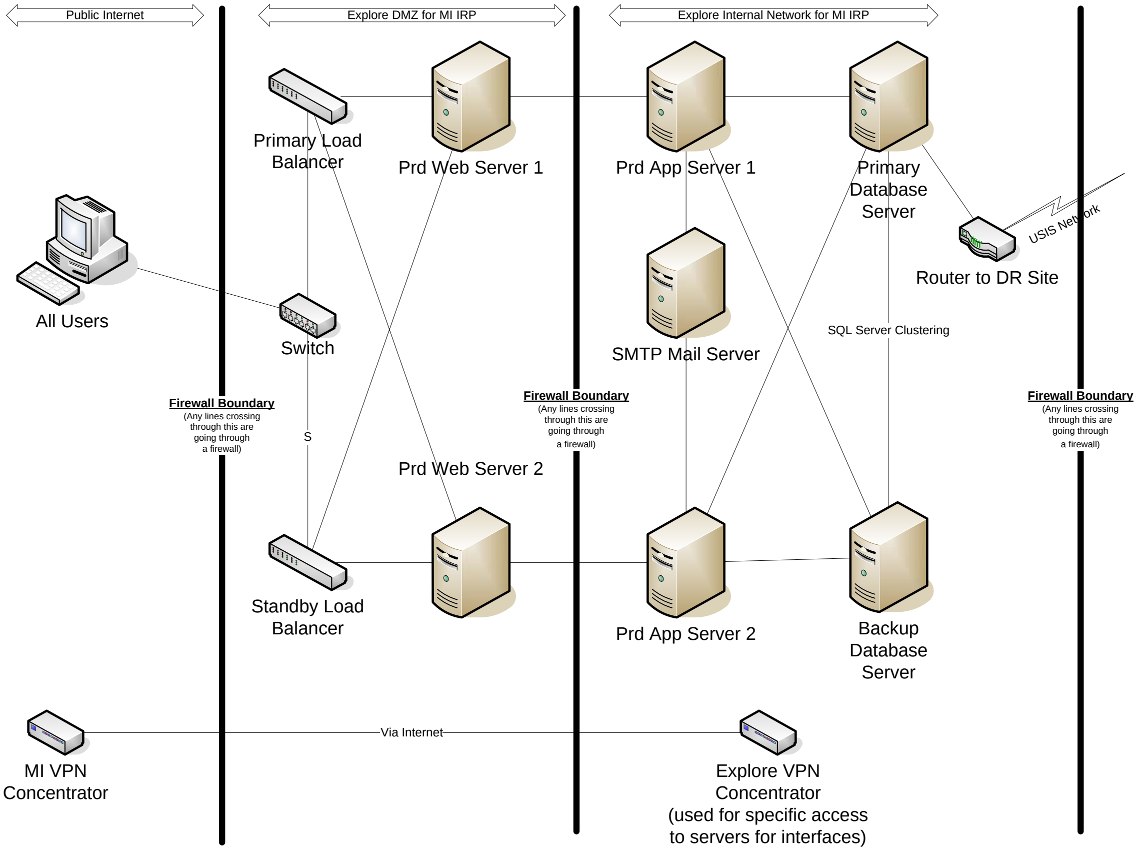
Location

If Michigan wishes to locate equipment in two different data centers, additional considerations apply. Network bandwidth needs to be considered. This may also affect the type of load balancer that is purchased since some load balancers are designed to balance traffic across a WAN and some are designed to balance it locally.

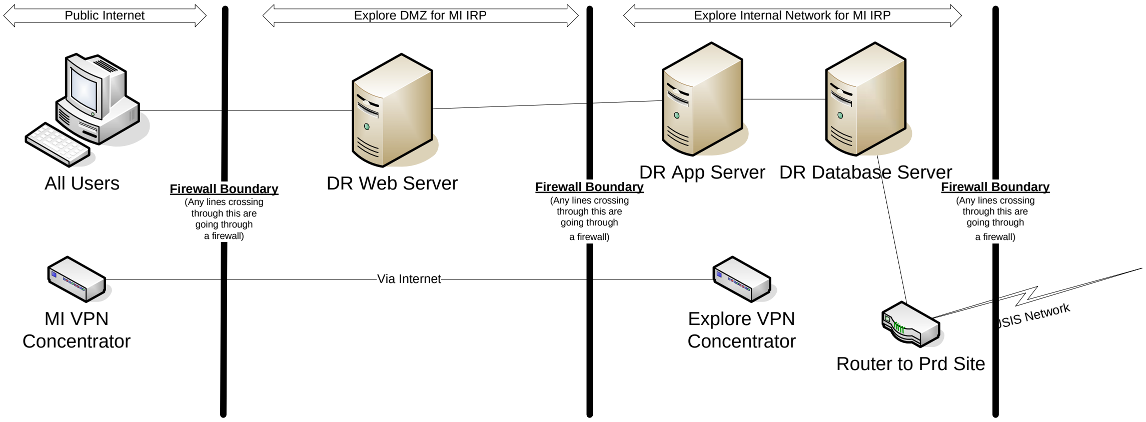
Scenarios

The following diagrams represent possible configurations that take into account business continuity.

Explore IRP Production Deployment Environment



Explore IRP Production Deployment Environment – Disaster Recovery Site



System Architecture Overview

The Explore IRP system is implemented in a multi-tier environment consisting of web server(s), application server(s) and database server(s). A description of common system components follows:

Firewall

The security policy at the State will need to be translated into an effective set of firewall rules and configuration files to act as a secure gateway between different networks. It should be configured to provide access to Explore IRP.

DMZ

A DMZ (demilitarized zone) refers to a host computer or network inserted as a “neutral zone” between an organization’s private network and the outside public network. Use of a DMZ prevents external users from getting direct access to a server that has organizational data. Users of the public network outside the organization can only access the DMZ host.

Web Server(s)

Web servers take requests from the client (through a browser session), process and forward the requests to the application server (where Explore IRP application software is housed) and returns the information to the client.

Application Server(s)

The Explore IRP application software will reside on application servers with replication enabled. Application Server(s) maintain the business rules to direct the user to the appropriate web page via the web server. Application clustering in conjunction with web-server load balancing provides necessary scalability and fail-over capabilities. We also use the application servers for processing scheduled batch jobs (i.e. printing of renewals, batch interfaces, generated clearinghouse file, etc.)

Database Server(s)

The Explore IRP database is hosted on a database server(s) running Microsoft® SQL Server 2005. Data is replicated to a backup database server for failover purposes. The backup server also servers a role as the database server for our test environments.

SMTP Mail Server

Access to a mail server is necessary for Explore IRP to send email notifications. Notifications are sent using the SMTP protocol.

DNS Server(s) (not shown, but recommended)

Required for internet access for carriers and licensing agents.

User Connectivity

Internal (Michigan) users access Explore IRP via the Internet (or possibly through intranet) as shown below. External users (carriers and service providers) access Explore IRP through the internet. Communications between the web browser and web server take place via HTTPS.

Structural Design (Database, Application Code, Business Logic, Programs)

Database

The Explore IRP database design includes several databases (all residing on one physical database server):

The Explore IRP main database where the majority of the transactional tables are located.

The Explore IRP fee database which houses fee charts for all of the jurisdictions.

The PRISM database which houses local copies of the PRISM Census, Target, and MCS-150 files.

The Warehouse database, where copies of selected data for ad hoc query purposes is maintained. The data warehouse is refreshed on a scheduled basis which will be determined during requirements gathering.

Application Code & Business Logic

Explore IRP business logic and application code is contained in SQL Server Stored Procedures, COM+ Components written in C#, and web pages written in C# served as ASP.NET. Business logic is separate from the web pages, keeping that logic focused on presentation. To support forms generation for cab cards, invoices, etc., Explore IRP reports that are defined in SQL Server Reporting Services. Explore IRP embraces W3C standards (i.e., XML, XSLT, XSL-FO, SOAP).

Programs

Our system consists of the IRP web site supplemented by batch applications for various processing functions including but not limited to:

- Batch interfaces to 3rd party systems such as Inventory, Clearinghouse, etc.
- Dynamic, monthly generation of renewal forms
- Dynamic generation of correspondence
- Dynamic generation of .PDF based cab cards and TOA’s.

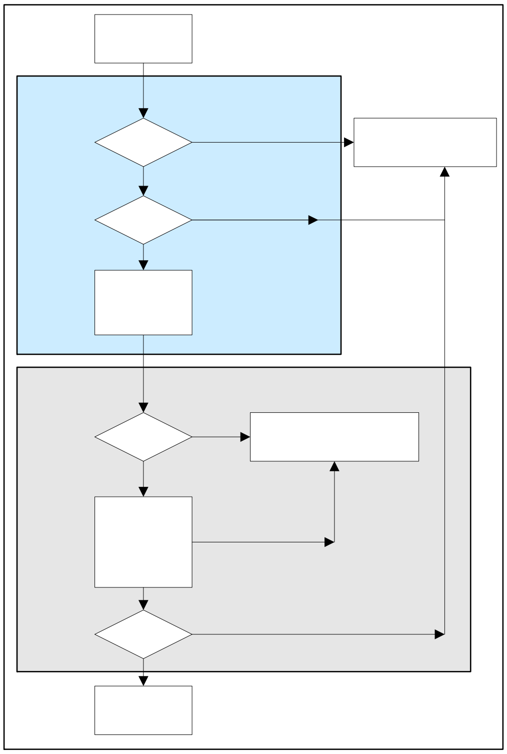
Security (Authentication, Authorization, Data Protection, Auditing, Physical and Network)

Explore IRP was designed to ensure that appropriate levels of security are implemented and maintained in order to maintain system integrity and to protect the integrity of jurisdiction data.

Security Architecture

The Explore IRP security architecture provides:

- **Individual Confidentiality and Privacy** – ensure information classified as protected by law or having the potential of being personal identifying information is processed in ways to prevent unauthorized access to the extent permitted by current technology.
- **System Integrity** – information is protected from tampering and unauthorized modification while in route and residing within the State's controlled infrastructure.
- **Application Availability** – authorized users of information technology resources can access appropriate resources in a timely manner. Procedures and standards resulting from this Enterprise Security Policy will address and support the security functions of:
- **Authentication –** certainty of source.
- **Authorization** -- granting of rights and privileges.
- **Administration** – security management.
- **Auditing –** enforcement and reporting.



Explore IRP was built on a multi-tier architecture, isolating the database layer, business layer and presentation layer among database servers, application servers and web servers. Explore IRP maintains all State data within the data layer of our architecture. Only the application server can access the database. The application server verifies that all incoming requests are from an authorized source. Communications between the web browser and web server take place via HTTPS.

Explore IRP authenticates users for secure web-based access through ASP.Net forms-based authentication. Web services are authenticated in the same manner. ASP.NET implements authentication using authentication providers, which are code modules that verify credentials and implement other security functionality such as cookie generation.

- **.NET Forms Authentication Module**. Using this causes unauthenticated requests to be redirected to a specified HTML form using client side redirection. The user can then supply login credentials, and post the form back to the server. Explore IRP authenticates the request (using application-specific logic). ASP.NET issues a cookie that contains the credentials or a key for reacquiring the client identity. Subsequent requests are issued with the cookie in the request headers, which means that subsequent authentications are unnecessary.

In addition to authentication, ASP.NET provides an impersonation mechanism to establish the application thread's security token. Obtaining the correct token is established by our use of IIS authentication and ASP.NET impersonation settings.

Explore IRP uses role-based security to control access to all aspects of the system. All users are assigned a user role. Setting up these roles is done through Explore IRP's user account maintenance functionality. Both internal (system administrators, staff, finance…) and external users (carriers and licensing agents) are maintained in this manner. To manage users, System administrators may disable users and reclassify their roles, and re-set user passwords for staff, carriers and licensing agents.

Explore's role-based security is hierarchical and will be configured for South Dakota specific user roles and requirements.

As a standard user roles will consist of Administrators, Power Users, Staff, Finance, Licensing Agents, Carriers, Auditor, Audit Reviewer and Read-Only. System Administrators and Power Users can create and disable user accounts at their level or below. Finance, Staff, Licensing Agents and Carriers can not create user accounts. Licensing Agents are restricted to viewing accounts for which they have permission to access. This is done through a unique, system generated access code that must be provided by the carrier. Once enabled, Carriers may disable access to licensing agents by simply selecting a link. Carriers are restricted to viewing and working on their own accounts. All changes, additions and removals are performed in real-time.

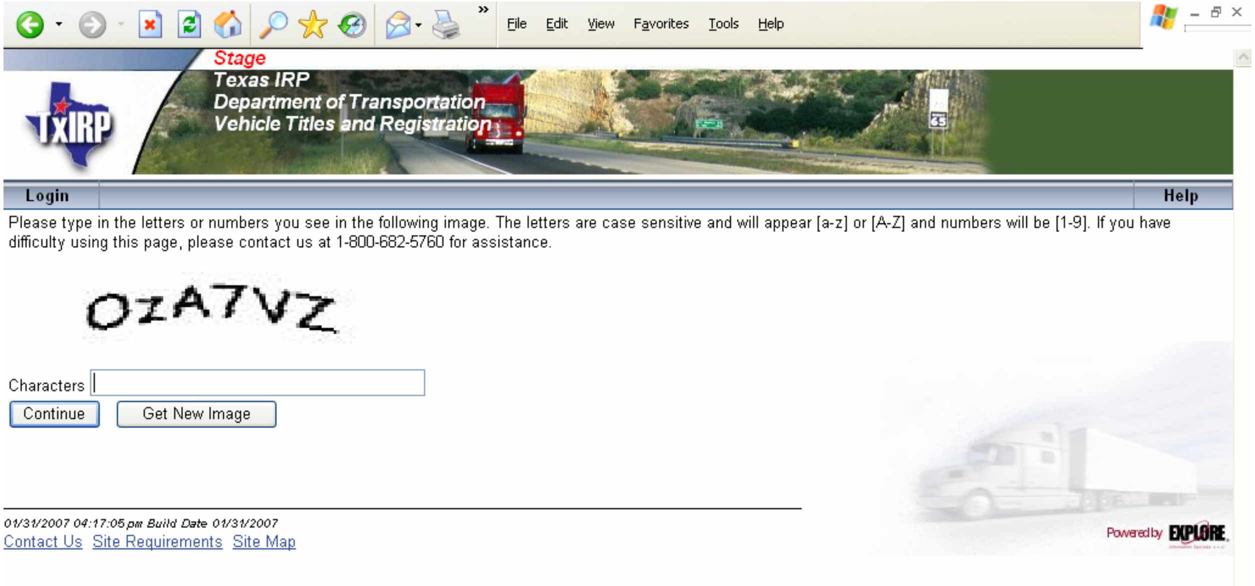
Explore's role-based security supports a multi-office/regional concept. If desired, all state roles can be established at the office level/region levels as well as the headquarters level. The multi-office/regional concept is brought forward in inventory management.

Based on user role, users may be restricted from performing specific events. This includes things like IRP functions, Intrastate functions, application specific actions (general, jurisdictions, weight groups, units, fee calculations, payments, and credentials), financial functions, inventory management functions, adjustment and correction functions (un-file, retractions).

If desired, Carriers may create their own user accounts. A secure 'Kaptcha' mechanism is place for new account validations. First time carrier users with IRP Accounts are required to enter a system generated account Access Code. This code is maintained in the IRP account record, and must initially be provided by State personnel to the carrier.

Carriers are restricted to viewing and working with their own accounts. Licensing Agents must be set up by a State administrator to access Explore IRP. Licensing

Agents may view/work with multiple carrier accounts if they have received authorization to do so. This is done via the account Access Code that must be provided to them. Carriers may disable licensing agent access at any time.



Please type in the letters or numbers you see in the following image. The letters are case sensitive and will appear [a-z] or [A-Z] and numbers will be [1-9]. If you have difficulty using this page, please contact us at 1-800-682-5760 for assistance.

Characters

01/31/2007 04:17:05 pm Build Date 01/31/2007

Explore IRP Authentication Methods and Practices

User account security is controlled by Microsoft Membership. System security, like database passwords, is based on encrypting the data with the RIJNDAEL algorithm using 256 bit keys. The master password itself is encrypted using Microsoft’s DPAPI.

Passwords must be 8 to 15 characters in length. Passwords must have at least one special character ~’!@#$%^&*()_-+=||{[}}]:;’”<,>.?/. Passwords must have at least one number. Passwords expire every 30 days (may be configured for the state) and must be reset by the user.

Digest authentication is used to encrypt the user's password information and provide a mechanism that helps prevent common server attacks (such as a replay attack).

Rigorous password security practices in place include:

- The login name is stored in the database in clear text.
- The password is stored in the database in encrypted text using a one-way hash.
- When a login is attempted, if the login name is matched but the password is invalid, a failed login attempt is logged for that account.
- Each User ID is required to be unique.
- User ID’s are unique in the system. The user is prevented from creating an account using an existing User ID.

Audit Trails

A variety of reports are accessible to system administrators that detail user activity. These include:

- The User Activity Report can be sorted by User ID with time stamps.

- The Applications Filed Report can be sorted by User ID.
- The Applications Paid Report can be sorted by User ID.
- The Applications in Progress Report can be sorted by User ID.
- Each application has View Work Activity link detailing who did each of the significant events on an application such as calculation of fees, filing, paying, etc.
- Each database action on transactional tables (not codes tables) has a trigger on it which stores the User ID that made each change and saves off prior values.
- Significant events are saved off in the various tables with the user session of who completed the transaction.

Explore IRP has audit trails that track the name, date and time for each action that results in a change in data. Each transaction is logged in the database. All logging is implemented by storing a new row in the database. Thus, no action will ever be overridden even if it is the same operation (for example, if a password was changed and then immediately changed again, there would be two rows in the log file showing both actions).

Only systems engineers and data base administrators have the capability to update these tables.

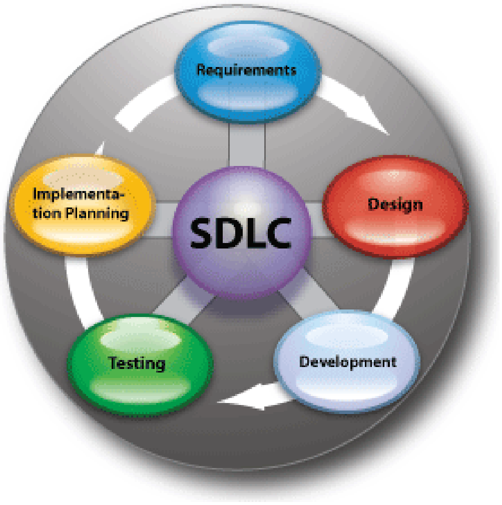
All logging is implemented by storing a new row in the database. Thus, no action will ever be overridden even if it is the same operation (for example, if a password was changed and then immediately changed again, there would be two rows in the log file showing both actions).

Controlled Migration Processes

Explore uses well defined, controlled processes for migrating code between stage, test and production servers.

Control Objective	Control	Y/N
1. Minimize opportunities for programmers to make unauthorized changes to production systems	Formal Change Request Process in place. Formal Request Tracker Management in place to identify and track requests	Y
2. Production transfer procedures reduce the risk of programmers introducing unapproved test versions into production systems	Use of Microsoft Visual Source Safe Code Library Software for control of code migrations. This prevents multiple developers from changing the same code module at the same time.	Y
3. Modifying the database should be controlled by change control procedures	Formal Change Request Process in place. Formal Request Tracker Management in place to identify and track requests	Y
4. Change Control Procedures include:		
4a. Management control	Method of requesting, authorizing, prioritizing, scheduling and communicating changes	Y
4b. Segregation of duties	Users initiate change, developers implement changes and moves code from stage to test. Tester test. Developers move test to production.	Y
4c. Documentation	Change request form Change control audit trails	Y
5. Back out procedures in the event of a failure during change	Procedures in place that identify back out and error resolution process. Version tracking capabilities of Microsoft Visual Source Safe enables Explore to restore applications to a point in time.	Y
6. Emergency move procedures to cover job aborts and special circumstances	Verification that emergency moves are necessary. Documentation in place	Y

All software customizations are performed using the Software Development Lifecycle Process (SDLC) to ensure the predictability and quality of enhanced software.


Requirements
Design
Development
Testing
Implementation Planning
SDLC